CITY OF SAN ANTONIO

Administrative Directive	**7.12 Data Governance**
Procedural Guidelines	Provides policies, processes, and standards that ensure the quality, integrity, security, availability, usability, and accessibility of the City's data assets while respecting residents' rights to privacy.
Department/Division	Information Technology Services Department
Revisions Date(s)	September 1, 2021
Last Reviewed	N/A
Owner	Chief Information Officer, Chief Data Officer

Purpose

Overview & Purpose of this Policy

The City of San Antonio offers online services, manages personal, operational and environmental data, and purchases technology to deliver effective public goods and services. As a provider of these public goods and services, it is the City of San Antonio's responsibility to establish a policy regarding how data is managed, secured, stored, and shared across City operations. This Data Governance AD sets forth policies, processes, and standards that ensure the quality, integrity, security, availability, usability, and accessibility of the City's data assets while respecting residents' rights to privacy. The policy is authorized by the City Manager and supported by the Data Governance Committee.

This policy applies to:

- All data processed, stored, and/or transmitted by a COSA Information Technology System(s)
- All COSA data processed, stored, and/or transmitted on personally owned devices also referred to as Bring Your Own Device ("BYOD")
- All data collected or maintained on a COSA owned and managed Network or authorized/contracted cloud platform by or on behalf of COSA in any form (electronic or hardcopy)

This policy shall be reviewed yearly by a Data Governance Committee. The Data Governance Committee is internal to the City of San Antonio and comprises of COSA staff. The purpose of the Data Governance Committee is to:

- Regularly review & revise the Data Governance AD
- Assesses the organization's progress towards its data governance goals

Policy

Roles & Responsibilities

This policy sets forth key overarching roles with regards to data. Each Department must identify three key roles for data management within their Department: Data Owner, Data Steward, and Subject Matter Expert. These roles are described below and **apply to City of San Antonio staff**:

- **Data Owner – Business Role**
  A Data Owner is the person at the Department Director's level who is responsible for the business relevance of the data generated in their organization, its operational value, its cleanliness, and overall data integrity. The Data Owner can also be a proxy owner of a dataset if their organization does not generate the data but are considered the authority of the data for the City of San Antonio (for example: US Census data).

- **Data Steward – Business Role**
  This role is delegated by the Data Owner to be responsible for data management and will establish appropriate governance and procedures required to ensure overall data integrity and reliability.

- **Subject Matter Expert (SME) – Business Role**
  A Subject Matter Expert is one who can answer detailed questions about the data, its meaning, its accuracy, and how it is generated.

- **Data Custodian – IT Role**
  ITSD application and database owners play the role of data custodians, as ITSD is responsible for the maintenance of underlying systems that power business applications. The Data Custodian ensures that systems are properly maintained with good change-management procedures, so that data integrity is maintained and free from system corruption.

Data Classification

The City of San Antonio recognizes the three data classifications outlined below. It shall be the responsibility of Data Owners to classify their data accordingly.

1. **Open Data**

   Open Data, also referred to as Public Data is all data not classified as Agency Sensitive Data or Confidential Data and may be released to the public. This information is subject to Open Records Requests (ORR). City Departments must provide such data on an official, City-designated Open Data Platform.

   For more information on Open Data, please refer to:
   1. The City of San Antonio Open Data Policy
   2. Open Data Procedures
   3. AD 1.31 Open Records (Texas Public Information Act) which places responsibility for developing and updating the Municipal Open Records Policy with the City Attorney's Office. This requirement includes any response to an Open Records Request ("ORR") whether or not the records are public under the Texas Public Information Act. All open records shall be reviewed by the department Data Owners prior to dissemination to reasonably assure that open records do not contain Confidential Data.

2. Agency Sensitive Data

This is data maintained by COSA that has agency-specific value and must be treated with special precautions or procedures to ensure confidentiality and integrity. The compromise or unauthorized release of Agency Sensitive Data could adversely affect the City's interests. Agency Sensitive Data may be classified as such by the Department's Data Owner. Agency Sensitive Data may be subject to disclosure or release under the Texas Public Information Act.

Examples of Agency Sensitive Data may include but are not limited to:

- COSA operational information
- COSA personnel records
- COSA information security configurations, data, and procedures
- Vendor bids and/or contract cost estimates among other sensitive data types

3. Confidential Data

Confidential Data may not be freely released due to its regulation by statutes, regulations, or industry standards. Includes Sensitive Personally Identifiable Information (SPII). Personally Identifiable Information (PII) is Confidential Data only if it includes one or more SPII elements.

We adhere to statutes, regulations, and industry standards that protect Confidential and sensitive data including, but not limited to:

- Data Governance Administrative Directive 7.12
- Data Security Administrative Directive 7.3
- The Privacy Act of 1974
- The Electronic Communications Privacy Act of 1986 ("ECPA")
- The Texas Public Information Act ("TPIA")
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- Health Information Technology for Economic and Clinical Health ("HITECH")
- The Texas Medical Privacy Act ("TMPA")
- The Payment Card Industry Security Standards ("PCI")
- The Criminal Justice Information Services ("CJIS") Security Policy
- City of San Antonio Ordinance 70508 (11-02-1989), naming the City Clerk as the City's Records Management Officer
- City of San Antonio Ordinance 72054 (08-09-1990), establishing the City's Records Management Program
- The Family Educational Rights and Privacy Act ("FERPA")

Personally Identifiable Information or PII, is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, or visitor to the U.S.

Sensitive Personally Identifiable Information, or SPII, is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, unfairness, and an increased risk to personal safety.

SPII is confidential. The release of SPII to the public is prohibited under the provisions of the Texas Public Information Act and other state and federal law. For more information regarding the protection of SPII, refer to Data Security Administrative Directive 7.3a.

Examples of SPII may include, but are not limited to, data types identified in Chapter 521 of the Texas Business and Commerce Code. For example, an individual's first name or first initial and last name in combination with personal identifying information, such as a social security number, driver's license number, or government-issued identification number, is not subject to public disclosure.

Below is a list of data that is always SPII:

- Social Security Numbers
- Alien Registration Numbers (A-numbers)
- Passport Numbers
- Driver's license Numbers or state identification numbers
- Biometric Identifiers (fingerprint, iris scan, voice print)
- Genetic data Network
- Physically secure hardcopy protected data in a locked drawer, file cabinet, desk, and/or safe

The following data is classified as SPII when linked with the person's name or other unique identifier, such as an address or phone number:

- Citizenship or Immigration status
- Criminal History
- Medical Information
- Bank Account or Routing/Transit Numbers
- Credit Card Numbers
- Income Tax Records
- Full Date of Birth
- Financial or Bank Account Numbers
- Fingerprint Identification Number ("FIN") or Student and Exchange

Data Privacy

The City of San Antonio respects the right to privacy across our applications, websites, and digital services. We minimize data collection to what is adequate, relevant, and necessary to achieve a clearly specified public interest. We will not collect or sell personal data without consent. We require that vendors awarded contracts with the City of San Antonio comply with the City's Data Governance AD 7.12. and Data Security Administrative Directive 7.3a.

What We Collect

Every Department in the City of San Antonio collects data to improve their services and build programming. Types of data City Departments may collect include:

- PII as required by law or necessary to render City services
- Voluntary Information through surveys and use of City services
- Website & Social Media Information
- Utility Information
- Digital Images or Videos

- Health Record Information
- Public Safety Information
- Financial and Payment Information
- Permitting Information
- Traffic & Environmental Data

All data collected by City of San Antonio departments is subject to classification as outlined above and is subject to Open Records Requests if not determined to be a protected class of data.

Data Security

As digital stewards, we protect data according to our Data Security Administrative Directive 7.3a.

Data Sharing

The City of San Antonio generally shares data with three groups:

1. **Between City Departments**, using, among other methods, the Enterprise Data Sharing Platform
2. **With external partners** using the Interlocal Data Sharing Agreement, Data Use and Confidentiality Agreements, and the Enterprise Data Sharing Platform
3. **With the public**, through ORR and the Open Data Portal (data.sanantonio.gov)

Sharing Data between City Departments

City Departments must curate their departmental data and make it accessible with the appropriate classification on an approved Enterprise Data Sharing Platform. City Staff must identify the appropriate roles and responsibilities specified in the "Data Platform Overview" document, available on the Enterprise Data Sharing Platform website accessible through the City's network. Once these roles are identified and allocated, assigned Departmental personnel can then start curating and publishing their data.

Sharing Data with External Partners

The City of San Antonio shares data with select external partners using the Interlocal Data Sharing Agreement (ILDSA), which the City was authorized to enter into through City Ordinance 2019-03-07-0186. The ILDSA was ratified by City Council in 2019, and specifies protocols for requesting data, roles and responsibilities, and necessary security protections when sharing data with external partners. For parties not covered under the ILDSA, Data Use and Confidentiality Agreements are negotiated on a case-by-case basis.

Sharing Data with the Public

The City of San Antonio shares Open Data with the public. The public can access Open Data on the City's Open Data Portal, https://data.sanantonio.gov. New data sets can be requested at https://data.sanantonio.gov/contact. Please refer to the City of San Antonio Open Data Policy and Open Data Procedures for detailed information about how to use the Open Data Portal, and its related policies. Open Records can be requested through the City's online Open Records portal at https://www.sanantonio.gov/opengovernment.

Data in City Operations

Departmental performance must be comprised of measures that contribute to the strategic goals of the City.

This policy sets forth the following requirements to standardize language and measures related to data and performance analytics in City operations, programs, and services.

1. When COSA departments report about their programs and projects both internally and externally, they must include a condensed statement describing each service or program they own/manage, clearly stating the public need addressed and the objective (goal) of said service or program.
2. City Departments must follow the guidelines listed in the *Data Governance Guidelines and Procedures* to define measures categorized as one of: Input, Output, Outcome, KPI-Quality, KPI-Cost, KPI-Cycle Time, KPI-Customer, KPI-Effectiveness.

Data in Procurement

In the event of technology purchases, or any purchase that collects or generates data, City Departments must strive for the following:

1. Ownership – The City of San Antonio will own all data collected or generated pursuant to an agreement. Generally, vendors may only use data for the purpose of (1) performing its obligation under the agreement; (2) providing maintenance and repairs to the City; and (3) if requested, improving its business operations and efficiencies.

2. Interoperability – Where possible, COSA should procure interoperable solutions that have common use to leverage the data produced, and reduce waste incurred by variability and duplication of effort.

3. Data Security Administrative Directive 7.3a – The contract between the City and the Vendor must reference the City's AD 7.3a to help assure the confidentiality, integrity, and availability of City-owned data.

Protected Health Information may not be disclosed to a Vendor unless, pursuant to and in accordance with HIPAA Regulations, the Vendor qualifies as a Business Associate, and the City and Vendor have executed a HIPAA Business Associate Agreement.

Guidelines for Internet of Things (IoT) Data

The City is committed to open and transparent data collection, transmission, processing and use for IoT deployments. City Departments must follow the guidelines listed in the *Data Governance Guidelines and Procedures* that apply to IoT deployments.

Guidelines for Automated Decision-Making

When using Automated Decision-Making, City Departments should follow the guidelines listed in the *Data Governance Guidelines and Procedures* or encourage that vendors providing the technology follow them.

Policy Applies To

☐ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	

Definitions

Agency Sensitive Data	The data classification for data that has agency-specific value, the confidentiality and integrity of which must be protected to avoid adversely affecting the agency's interests. Agency Sensitive Data may be subject to disclosure or release under the Texas Public Information Act unless the information is otherwise defined as confidential by law or another exception under the Act applies.
Automated Decision-Making	The process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.
Confidential Data	Data that may not be freely released due to its regulation by statutes, regulations, or industry standards. Includes Sensitive Personally Identifiable Information (see definition below).
Data Consumer	Anyone who has use or interest in a data set published by City Departments or external agencies with whom the City has a data sharing agreement.
Data Custodian	ITSD application and database owners who ensures that systems are properly maintained with good change-management procedures, so that data integrity is maintained and free from system corruption.
Data Governance	A set of policies, processes, and tools that ensure data quality, accessibility, usability, integrity, and the overall readiness of data that is used to make business decisions intended to create, improve or sustain services and products.
Data Owner	A Data Owner is the one who is responsible for the business relevance of the data generated in his/her organization, its operational value, its cleanliness, and overall data integrity. The Data Owner can also be a proxy owner if their org does not generate the data, but they are actually the authority that speaks to it in City of San Antonio.
Data Stakeholders	Anyone who can impact, or be impacted by, or have interest in the data.
Internet of Things (IoT)	The Internet of Things refers to a network of devices, sensors, or software applications that exchange information over the internet. For example, installing a sensor on a streetlight that collects air quality data that is transmitted over the internet back to the City of San Antonio, is an IoT deployment.
Open Data	The data classification for all data not classified as Confidential or Agency Sensitive and may be released to the public.
Open Data Portal	A web portal maintained by or on behalf of COSA that will be the repository for COSA's Open Data. The portal provides access to standardized data that can be easily retrieved, downloaded, sorted, searched, analyzed, redistributed and re-used by the public.
Personally Identifiable Information ("PII")	The data classification for information that alone or in conjunction with other information identifies an individual, including an individual's: (i) name, social security number, date of birth, or government-issued identification number; (ii) mother's maiden name; (iii) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (iv) unique electronic identification number, address, or routing code; and (v) telecommunication access device, including a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, or other telecommunications service, equipment, or instrument identifier or means of account access that alone or in conjunction with another telecommunication access device may be used to (a) obtain money, goods, services, or other thing of value; or (b) initiate a transfer of funds other than a transfer originated solely by paper instrument.

Record Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction pursuant to the Local Government Record Retention Schedules issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Texas Government Code.
Sensitive Personally Identifiable Information ("SPII")	The data classification for information that has not been made lawfully available to the public from the federal, state, or local government, including (i) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:(a) social security number; (b) driver's license number or government-issued identification number; or (c) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (ii) information that identifies an individual and relates to: (a) the physical or mental health or condition of the individual; (b) the provision of health care to the individual; or (c) payment for the provision of health care to the individual.
Subject Matter Expert (SME)	A Subject Matter Expert is one who can answer detailed questions about the data, it's meaning, its accuracy, and how it is generated.

Policy Guidelines

Policy guidelines and important guidance information are included in *Data Governance Guidelines and Procedures* and *Attachment A: Principles of Data-Informed Government.*

Procedures (if necessary)

Procedures are included in *Data Governance Guidelines and Procedures* and *Attachment A: Principles of Data-Informed Government.*

Roles & Responsibilities

Employees	• Understand the policies, procedures, and standards that are in place for data used in their daily work and learn how to properly use and protect data as an asset. • Comply with the Data Governance AD when performing daily tasks. • Enforce Data Governance AD standards in procurement processes with Vendors • Get trained on and use the Enterprise Data Sharing Platform. • Share any data governance concerns with City Leadership.
Department Directors	• Assign up to two Data Stewards responsible for ensuring compliance with the AD by managing and maintaining data within each department. • Understand the role data plays within the organization in order to advance a data-informed culture at COSA. • Ensure staff is aware of the Data Governance AD and adhere to Data Governance best practices, and this AD. • Support process and data-cleanliness audits.
Data Owner	• A Data Owner is the person at the Department Director's level who is responsible for the business relevance of the data generated in their organization, its operational value, its cleanliness, and overall data integrity. The Data Owner can also be a proxy owner of a dataset if their organization does not generate the data but are considered the authority of the data for the City of San Antonio (for example: US Census data).

Data Steward	• This role is delegated by the Data Owner to be responsible for data management and will establish appropriate governance and procedures required to ensure overall data integrity and reliability.
Subject Matter Expert	• A Subject Matter Expert is one who can answer detailed questions about the data, its meaning, its accuracy, and how it is generated.
Data Custodian	• ITSD application and database owners play the role of data custodians, as ITSD is responsible for the maintenance of underlying systems that power business applications. The Data Custodian ensures that systems are properly maintained with good change-management procedures, so that data integrity is maintained and free from system corruption.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department.

CITY OF SAN ANTONIO

EMPLOYEE ACKNOWLEDGMENT FORM FOR

ADMINISTRATIVE DIRECTIVE 7.12
Data Governance

Employee:

I acknowledge that on _____, 20____, I received a copy of Administrative Directive 7.12 Data Governance, and was given the opportunity to ask questions or contact my Human Resources Representative.

_____ _____
Employee Name (Print) Department

_____ _____
Employee Signature Employee SAP ID Number

Attachment A
Personnel File (original)